GIBSON DUNN & CRUTCHER LLP
ETHAN D. DETTMER, SBN 196046
edettmer@gibsondunn.com
ABIGAIL A. BARRERA, SBN 301746
abarrera@gibsondunn.com
ASHLEY J. HODGE, SBN 287653
ahodge@gibsondunn.com
ANTHONY D. BEDEL, SBN 324065
tbedel@gibsondunn.com
555 Mission Street, Suite 3000
San Francisco, CA 94105
Telephone: 415.393.8200
Facsimile: 415.393.8306

GIBSON, DUNN & CRUTCHER LLP
ALEXANDER H. SOUTHWELL (*pro hac vice*)
asouthwell@gibsondunn.com
200 Park Avenue, 48th Floor
New York, NY 10166
Telephone: 212.351.4000
Facsimile: 212.351.4035

Attorneys for Defendant PLAID INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

IN RE PLAID INC. PRIVACY LITIGATION

THIS DOCUMENT RELATES TO:

ALL ACTIONS

Master Docket No. 4:20-cv-03056-DMR

DEFENDANT PLAID INC.'S NOTICE OF MOTION, MOTION TO DISMISS, AND MEMORANDUM OF LAW IN SUPPORT OF MOTION TO DISMISS PLAINTIFFS' CONSOLIDATED AMENDED COMPLAINT

ORAL ARGUMENT REQUESTED

Action Filed: May 4, 2020

Judge: Hon. Donna M. Ryu

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that, as soon as practicable after briefing is completed on Defendant Plaid Inc.'s ("Plaid") Motion to Dismiss Plaintiffs' Consolidated Amended Complaint ("CAC"), Plaid requests to be heard before the Honorable Magistrate Judge Donna M. Ryu, in Courtroom 4, Third Floor, of the United States District Court for the Northern District of California, located at 1301 Clay Street, Oakland, CA 94612. The current schedule, as set forth in the July 29, 2020 Order (ECF No. 57) sets the completion of all briefing on these issues for 21 days after Plaintiffs' Opposition to Plaid's Motion is filed. The May 27, 2020 Order (ECF No. 36) further provides "[t]he Court will set a hearing on the motion upon completion of the briefing, if necessary."

Pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), Defendant Plaid will, and hereby does, move the Court for an Order dismissing with prejudice Plaintiffs' CAC for, *inter alia*, the following reasons:

- Plaintiffs lack standing under Article III.
- Most of Plaintiffs' claims are time-barred.
- Plaintiffs' equitable claims and remedies fail because Plaintiffs have an adequate remedy at law.
- Plaintiffs' claims fail as a matter of law because they do not state a claim upon which relief may be granted.

Plaid's Motion is based upon this Notice of Motion and Motion and Memorandum of Points and Authorities, the Declaration of Ethan D. Dettmer and its attachments, and Plaid's Request for Judicial Notice, as well as the records, pleadings, and papers on file in this action, and upon such other matters as may be presented before or at the time of the hearing on this Motion, which the Court will set, "upon completion of the briefing, if necessary." ECF No. 36 at 4.

Dated: September 14, 2020

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

/s/ Ethan D. Dettmer
By: Ethan D. Dettmer

Attorneys for Defendant Plaid Inc.

TABLE OF CONTENTS

TABLE OF CONTENTS (*continued*)

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES (*continued*)

Page(s)

TABLE OF AUTHORITIES (*continued*)

Page(s)

TABLE OF AUTHORITIES (*continued*)

Page(s)

TABLE OF AUTHORITIES (*continued*)

Page(s)

TABLE OF AUTHORITIES (*continued*)

Page(s)

TABLE OF AUTHORITIES (*continued*)

Page(s)

TABLE OF AUTHORITIES (*continued*)

Page(s)

TABLE OF AUTHORITIES (*continued*)

Statutes

Other Authorities

TABLE OF AUTHORITIES (*continued*)

Treatises

Regulations

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Consumers and small businesses rely on digital applications ("apps") for financial services now more than ever before. These apps help end users[1] transfer money, streamline loan applications, create budgets, save for retirement, and more. But before end users can reap the benefits of such apps, they often need to be able to share their financial data from their bank or other financial accounts with their selected apps. That is where Plaid comes in: Plaid provides technology that enables end users to connect their financial accounts to the apps of their choosing. By enabling end users to control and share their data, Plaid makes it possible for end users to use the financial services provided by their chosen apps, thereby democratizing access to financial services.

Stripped of its baseless rhetoric, Plaintiffs' Consolidated Amended Complaint ("CAC") concedes that end users should be able to control their financial data and share it as they choose. Indeed, Plaintiffs allege that they themselves exercised that control by choosing to connect their financial accounts to certain apps to manage one aspect of their financial lives: sending and receiving payments. The crux of the CAC is Plaintiffs' alleged lack of understanding of Plaid's data collection and handling practices. But Plaid makes its data policies and practices clear on its website and in its End User Privacy Policy (the "Privacy Policy," which is incorporated by reference in the CAC), to which all Plaintiffs had reasonable access, consistent with applicable legal standards. Plaid makes clear in its Privacy Policy that—contrary to Plaintiffs' implausible claim—it does not obtain data without consent, and does not sell or rent personal information. Plaintiffs have control over their financial data—if Plaintiffs do not want the benefit of Plaid's service, they do not have to use it and can turn it off at any time. The CAC should be dismissed in full and with prejudice because Plaid's disclosures undermine all their claims.

Plaintiffs' CAC fails for multiple additional reasons, including, *inter alia,* that:

- While they vaguely allege linking their bank accounts to certain apps, Plaintiffs do not allege they used Plaid to do so. Venmo, for example (which every named Plaintiff supposedly used), allows users to link accounts *without* using Plaid (and can even be used without linking any financial account at all). Plaintiffs' failure to allege their use of Plaid in the linking process—let alone any facts about such linking—is fatal to their claims.

[1] For purposes of this Motion, "end user" refers to an individual consumer, unless otherwise noted.

- Plaintiffs do not allege facts to show any actual or imminent concrete economic or non-economic harm as is required to establish Article III standing. Plaintiffs do not allege asking Plaid to delete their data (to the extent it has their data in the first place), utilizing the option to link their accounts without Plaid, or disabling the connections between their banks and apps. Plaintiffs' claims of "harm" are not plausible, nor is their self-serving claim that they would not have connected their accounts, if they had known about Plaid's practices.
- Most of the Plaintiffs' claims are time-barred.
- Plaintiffs' equitable claims and requests for relief fail because they have (and allege) an adequate legal remedy.
- Plaintiffs fail to allege all the required elements of *any* of their ten causes of action.

Because Plaintiffs' claims fail for numerous, independent reasons that cannot be remedied, the CAC should be dismissed with prejudice. Leave to amend should be denied given Plaintiffs have already had ample time to investigate and, even more importantly, to amend and consolidate their five complaints. If Plaintiffs could not come up with a viable claim with 12 law firms, 19 named plaintiffs (some of whom were dropped from the CAC), and 112 pages and 378 paragraphs of allegations, they will not be able to do so in the future. Further leave to amend would be futile.

II. ISSUES TO BE DECIDED

1. Whether the CAC should be dismissed because Plaintiffs lack standing under Article III.
2. Whether most of Plaintiffs' claims should be dismissed because those claims are time-barred.
3. Whether the equitable claims and remedies fail because Plaintiffs have adequate legal remedies.
4. Whether the CAC should be dismissed because Plaintiffs' claims fail as a matter of law.

III. FACTUAL BACKGROUND

A. Plaid provides technology that enables end users to connect their financial accounts to the apps and services of their choosing.

End users are increasingly turning to digital apps to manage their financial lives;[2] these apps allow them to do things like transfer money, manage spending, and save for retirement. In order to provide financial services to end users, many of these apps need data from end users' bank or other financial accounts and thus may require end users to connect those accounts to their chosen apps.

[2] *See* "A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation," U.S. Dept. of the Treasury, July 2018 at 18, *available at https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf* ("[U]p to one-third of online U.S. consumers use at least two fintech services—including financial planning, savings and investment, online borrowing, or some form of money transfer and payment.").

Plaid's technology is one method that enables end users to do this. When end users choose to connect their financial accounts to an app through Plaid, Plaid will, ***at the end users' direction***, collect data from their accounts and share it with the end user's chosen app. Contrary to Plaintiffs' baseless claims, Plaid does not collect or share data without permission; the connection between their apps and their financial accounts is only made when Plaintiffs choose to make it. By delivering end-user-permissioned access to financial account data, Plaid enables apps to build and provide better financial management tools for their end users. Indeed, taking advantage of such financial management tools is exactly what Plaintiffs concede they were trying to do when they signed up to use—and chose to allegedly link their financial accounts to—Venmo, Cash App, and Coinbase, apps that would allow them to easily transfer money.

B. Plaid's policies and practices promote transparency and safeguard end-user data.

Plaid's Privacy Policy clearly discloses its data-processing practices. Plaintiffs' tabloid-ready claim that Plaid "sells the consumer banking data it collects" (CAC ¶ 59) is repeated throughout the CAC.[3] Plaintiffs appear to rely on repetition as a substitute for sufficient pleading—likely because they lack any facts to support their baseless accusation. However, such repetition of a conclusory, legally insufficient allegation—without a single fact to support it—does not meet the pleading requirements of Rule 8 or Rule 9 and cannot withstand scrutiny on a Motion to Dismiss. Although Plaid does not sell consumer data, more importantly for this Motion to Dismiss, Plaintiffs have not offered a single fact to support their accusation, and Plaid's Privacy Policy makes clear that Plaid does "not sell or rent personal information" that it collects. Ex. A at 5.[4] Further, Plaid's Privacy Policy expressly discloses how Plaid collects, uses, and shares end-user information in its

[3] Plaintiffs' reliance on Visa's acquisition of Plaid is misleading. Subject to regulatory approvals and other customary closing conditions, Visa will acquire Plaid as an ongoing business; the data is necessary for Plaid's business to continue to function. In any event, Plaid expressly notifies end users—as many online services do—that their data may be shared "[i]n connection with a change in ownership or control of all or part of [its] business" such as an acquisition. *See* Ex. A at 5 (all exhibit references refer to the exhibits attached to the Declaration of Ethan D. Dettmer).

[4] Plaintiffs grossly mischaracterize Plaid's business, advancing rank speculation and relying on misleading interpretation to falsely portray Plaid's business. As just one example, the CAC quotes a former Plaid programmer speculating that Plaid could theoretically monetize data it collects, but notably not claiming that Plaid does sell this data. *Id.* ¶ 63. As Plaid makes clear, it does not sell data. *See* Ex. A at 5. In any event, the false assertion that Plaid sells data is not an element of, or material to, any of Plaintiffs' claims and thus not germane to this Motion.

possession to operate, improve, develop, and protect its services, and as described in the Privacy Policy.[5]

Plaintiffs misrepresent Plaid's Privacy Policy disclosures. In alleging various failures to disclose, Plaintiffs repeatedly mischaracterize Plaid's statements in its Privacy Policy, as illustrated by the chart below, which juxtaposes Plaintiffs' baseless allegations of omission with the express disclosures in Plaid's Privacy Policy. Where, as here, conclusory allegations are contradicted by documents incorporated into the complaint (and of which judicial notice should be taken), such allegations need not be accepted as true and can be disregarded. *In re Am. Apparel, Inc. S'holder Litig.*, 855 F. Supp. 2d 1043, 1060 (C.D. Cal. 2012) (quoting *Steckman v. Hart Brewing Inc.*, 143 F.3d 1293, 1295 (9th Cir. 1998)) ("The court is 'not required to accept as true conclusory allegations which are contradicted by documents referred to in the complaint.'"):

Information Plaintiffs Allege Plaid's End User Privacy Policy Fails To Disclose	**Plaid Privacy Policy's Actual Disclosures (Contrary To Plaintiffs' Allegations)**
"Plaid collects consumer bank login information directly[.]" CAC ¶ 74(h).	Plaid expressly discloses, "***[W]e collect identifiers and login information required by the provider of your account***, such as your username and password, or a security token. In some cases, we also collect your phone number, email address, security questions and answers, and one-time password (OTP) to help verify your identity before connecting your financial accounts." Ex. A at 2 ("Information you provide") (emphasis added).
"Plaid uses bank login information to access consumers' accounts." *Id*.	Plaid expressly discloses, "When providing this information, you give the developer and Plaid the authority to act on your behalf ***to access and transmit your End User Information*** from the relevant bank or other entity that provides your financial accounts." *Id*. (emphasis added).
"Plaid collects all available private financial and other identifying data from every available account once it accesses the 'linked' account[.]" *Id*.	Plaid expressly discloses, "The data collected from your financial accounts includes information from ***all your accounts*** (*e.g.*, checking, savings, and credit card) ***accessible through a single set of account credentials***." *Id*. at 3 (emphasis added). Further, the Privacy Policy makes clear, contrary to Plaintiffs' conclusory, legally insufficient allegation, "The information we receive from the financial product and service providers that maintain your financial accounts ***varies depending on the specific Plaid services developers use to power their applications, as well as the information made available by those providers***." *Id*. at 2-3 ("Information we collect from your financial accounts") (emphasis added).
"Plaid sells the consumer banking data it collects to its clients[.]" *Id*.	Contrary to Plaintiffs' legally insufficient allegation, Plaid expressly discloses, "***We do not sell or rent personal information*** that we collect." *Id*. at 5 ("How We Share Your Information") (emphasis

[5] Because Plaintiffs' "claim depends on the contents of [the] document" (*Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005) (internal citation omitted)), the Court may properly consider it.

	added). To the extent Plaintiffs are claiming that Plaid wrongfully shared end user data with the developer of the end user's chosen app, Plaid specifically discloses that it shares end-user data "[w]ith the developer of the application you are using and as directed by that developer." *Id*.
"Plaid otherwise uses and monetizes the consumer banking data it collects[.]" *Id*.	Plaid expressly discloses its uses of data in its Privacy Policy: "***We use your End User Information for a number of business and commercial purposes***, including to operate, improve, and protect the services we provide, and to develop new services." *Id*. at 4 ("How We Use Your Information") (emphasis added) (listing purposes for which the data is used). Further, contrary to Plaintiffs' vague and legally insufficient allegation about monetization, the Privacy Policy expressly states, "***We do not sell or rent personal information*** that we collect." *Id*. at 5 ("How We Share Your Information") (emphasis added).
"Plaid stores the consumer banking data it collects[.]" *Id*.	Plaid expressly discloses, "We retain End User Information for no longer than necessary to fulfill the purposes for which it was collected and used, as described in this Policy, unless a longer retention period is required or permitted under applicable law. As permitted under applicable law, ***even after you stop using an application or terminate your account with one or more developer, we may still retain your information*** (for example, if you still have an account with another developer)." *Id*. ("Our Retention Practices") (emphasis added).
"Venmo purchases, uses, and stores the consumer banking data collected by Plaid[.]" *Id*.	Again, contrary to Plaintiffs' wholly unsupported, legally insufficient allegation, Plaid expressly discloses, "***We do not sell or rent personal information*** that we collect." *Id*. ("How We Share Your Information") (emphasis added). The remainder of the information Plaintiffs allege Plaid fails to disclose is expressly disclosed: "We share your End User Information for a number of business purposes: ***With the developer of the application you are using*** and as directed by that developer (such as with another third party if directed by you)." *Id.* (emphasis added).
"Plaid continues to access accounts and collect, sell and use consumer banking data after the initial connection is made, regardless of whether the consumer continues using the Venmo app[.]" *Id*.	Plaid expressly discloses, "As permitted under applicable law, ***even after you stop using an application or terminate your account with one or more developer, we may still retain your information*** (for example, if you still have an account with another developer)." *Id*. ("Our Retention Practices") (emphasis added). Plaid expressly discloses, "***We do not sell or rent personal information*** that we collect." *Id*. (emphasis added).
"Plaid does not exercise adequate oversight over how consumer banking data is stored or used after it sells that data to Venmo[.]" *Id*.	With respect to Plaintiffs' baseless, legally insufficient allegation about sale of data, Plaid expressly discloses, "***We do not sell or rent personal information*** that we collect." *Id*. Further, Plaid's Privacy Policy expressly discloses, "Please note that this Policy only covers the information that Plaid collects, uses, and shares. ***It does not explain what developers do with any End User Information we provide to them*** (or any other information they may collect about you separately from Plaid). This Policy also does not cover any websites, products, or services provided by others. ***We encourage you to review the privacy policies or notices of developers or those third parties for information about their practices***." *Id*. at 2 ("About this Policy") (emphasis added).

Plaid has enacted robust security practices to protect end users' data. Plaid's security program is designed to meet or exceed industry standards, using strong, multi-factor authentication

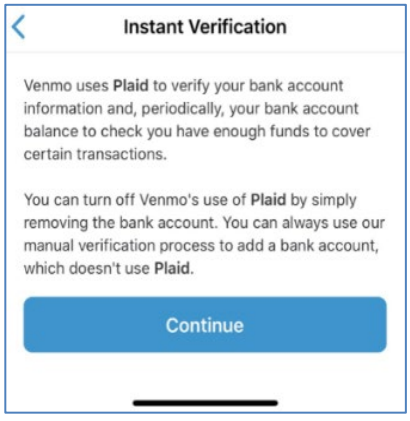
for critical internal systems and continuously monitoring the Plaid API for potential security breaches.[6]

C. End users connecting through Plaid learn about Plaid's role and its Privacy Policy.

Plaintiffs try to make much of "Plaid Link," which is Plaid's technology through which apps enable end users to connect their financial accounts to their apps so they can use financial services provided by those apps. Although the named Plaintiffs do not even allege they linked accounts through Plaid, they spend several pages falsely characterizing Plaid Link as a tool that imitates bank login screens to "trick" end users into providing their login credentials. *See*, *e.g.*, CAC ¶¶ 67-75.

In describing the experience of connecting financial accounts to the Venmo app through Plaid Link, Plaintiffs concede that end users are told their chosen app "uses Plaid to link to your bank," and that by choosing to "continue" (*i.e.*, to engage with and proceed through the linking process), end users consent to Plaid's Privacy Policy. *See*, *e.g.*, *id.* ¶ 67. Indeed, Plaintiffs even include a screenshot of the flow for Venmo, the first screen of which expressly discloses to end users that "Venmo uses Plaid to link your bank," and, directly above the "Continue" button, explains to end users that "[b]y selecting 'Continue' you agree to the Plaid End User Privacy Policy." *Id.* ¶ 68. Plaid's Privacy Policy is linked in the disclosure directly above the "Continue" button that users must press to continue the linking process, and end users can review the Policy in its entirety within the Plaid Link flow. *Id.*

Notably, Plaintiffs do not acknowledge that there is another important screen in the current Venmo flow *before* the one Plaintiffs display (shown at right).[7] The screen Plaintiffs fail to acknowledge in their CAC explains in plain language—in addition to the disclosure discussed above—what Plaid does, that end users can choose to link their accounts to Venmo without Plaid, and that they can always "turn off Venmo's use of Plaid." Thus, it is clear to Venmo users (which include each named Plaintiff)—on two separate screens—what Plaid's role is in



[6] *See* Plaid Inc., "Security," *available at* http://Plaid.com/security/ (last visited Sept. 14, 2020).

[7] This image is from the Venmo app. The complete document—the flow that end users experience when connecting their financial accounts through Plaid—is contained in Exhibit E.

the account-linkage process, and that users can choose *not* to use Plaid to connect their financial accounts. But Plaintiffs simply ignore the disclosure of Plaid's role and the clearly described options presented to end users who wish to use Venmo without Plaid. Further, Plaintiffs do not allege disconnecting their accounts, or asking Plaid to delete their data, despite claiming they "would not have connected" their accounts had they known about Plaid's role. *Id.* ¶¶ 105, 116, 126, 135, 145, 155, 164, 173, 183, 194, 204.

After clicking the "Continue" button and choosing to proceed with linking their financial accounts through Plaid Link, end users then enter the login credentials for their financial account, which authenticate the end users' ownership of the account, and also "give the developer [*i.e.*, the app] and Plaid the authority to act on [the end users'] behalf to access and transmit [the end users'] End User Information from the relevant bank or other entity that provides [the end users'] financial accounts." Ex. A at 2 ("Information you provide"). Plaintiffs claim that Plaid Link is inferior to an authentication protocol called "OAuth" and (as previously noted) intended to mimic the look and feel of a bank to "trick" end users into providing their login credentials. *Id.* ¶¶ 35-37. ***This is a red herring.*** The vast majority of financial institutions have not implemented (and do not have the technological resources to implement) an OAuth protocol, which entails building and providing a dedicated API endpoint to enable end users to share their data after the institution itself verifies the user's identity. Plaid aims to provide *all* end users—regardless of the level of sophistication of the end user's financial institution—access to the fintech marketplace, and Plaid successfully does this by streamlining the authentication and authorization process for end users through Plaid Link.

D. The named Plaintiffs do not claim they linked their accounts through Plaid.

Plaintiffs allege that, at some point over the last six years, they "signed up to use" certain apps that allow end users to link their financial accounts to apps through Plaid. *See*, *e.g.*, *id.* ¶¶ 130, 140, 188-189. However, the fact that a certain app makes account linkage available through Plaid does not mean the only method of account linkage is through Plaid. As shown in the Venmo illustration above, Venmo allows end users to link their accounts through methods other than Plaid (and to use the app without linking any account at all). Critically, here, Plaintiffs do ***not*** allege that they *in fact* linked their financial accounts to their chosen apps (including Venmo) ***using Plaid***. Plaintiffs have

simply not implicated Plaid in the conduct they complain of (which fatally undermines all of their claims, as well as their ability to establish any alleged harm caused by Plaid).

IV. LEGAL ARGUMENT

A. Plaintiffs lack Article III standing to pursue their claims.

To pursue their purported claims, Plaintiffs must "set forth facts sufficient to satisfy [the] Article III standing requirements" (*Whitmore v. Ark.*, 495 U.S. 149, 155-56 (1990)), which "pertain to a federal court's subject-matter jurisdiction" (*White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000)). Article III requires Plaintiffs to plead facts sufficient to show: (1) an injury in fact; (2) a causal connection between the injury and the conduct complained of; and (3) a substantial likelihood that the requested relief will remedy the alleged injury in fact. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992). In addition, "named plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.'" *Lewis v. Casey*, 518 U.S. 343, 357 (1996) (citations omitted). Plaintiffs have not pled—and cannot plead—facts sufficient to satisfy Article III standing requirements and their lawsuit must be dismissed for that reason alone.

1. Plaintiffs fail to sufficiently plead an injury in fact.

To satisfy the injury-in-fact element of Article III standing, a plaintiff must plead an injury that is "concrete in both a qualitative and temporal sense" and "actual or imminent, not conjectural or hypothetical." *Whitmore*, 495 U.S. at 155 (internal citations and quotations omitted); *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). Despite spending 137 paragraphs trying to manufacture a tale of such injury, Plaintiffs fail to do so. They allege only legally insufficient, hypothetical harms and cannot articulate any concrete, actual or imminent harm because they have not suffered one.

a. Plaintiffs fail to sufficiently plead any "Economic Damages."

"Loss of Valuable Indemnification Rights." Plaintiffs do not allege they have experienced any fraudulent charge—let alone that they have been denied indemnification rights by any banks. Instead, Plaintiffs allege their decision to connect their financial accounts to various apps *could* cause them to lose indemnification rights under banking laws (Regulation E) *if*, at some unspecified point in the future, they experience a fraudulent charge as a result of connecting their accounts through

Plaid and the financial institutions happen to determine that "the[ir] provision of login credentials" to Plaid constitutes "a grant of 'authority' to conduct funds transfers." CAC ¶¶ 215-224. Notably, Plaintiffs do not allege they have actually experienced any fraudulent charge—let alone that they have been denied indemnification rights by any banks. Such allegations are insufficient, as the "test is *actuality*, *not hypothetical speculations* concerning the possibility of future injury." *Reilly v. Ceridian Corp*., 664 F.3d 38, 43 (3d Cir. 2011) (emphasis added) (hypothetical chain of "ifs," after data breach, was insufficient to constitute Article III injury because "we cannot now describe how Appellants will be injured in this case without beginning our explanation with the word 'if.'").

Here, the hypothetical nature of Plaintiffs' purported harm is underscored by the fact that such harm could only be realized if a chain of at least six events (*not a single one of which Plaintiffs allege has actually occurred* and which are predicated in large part upon the unpredictable actions of third parties) all happened to take place at some point in the future: (1) a hacker would need to gain access to Plaintiffs' financial data, (2) while that data was being stored or transmitted by Plaid, and (3) the hacker would then need to use that data to make an unauthorized transfer of funds from Plaintiffs' bank account; (4) Plaintiffs would then need to report the hypothetical unauthorized transfer within the required timeframe to their financial institution, (5) which, in turn, would need to deem Plaintiffs' provision of their login credentials to Plaid as a grant of authority to conduct funds transfers and (6) based thereon, refuse to indemnify Plaintiffs.[8] Plaintiffs do not allege even the first step in this long chain of improbable and speculative contingencies, much less all of them. This "highly attenuated chain of possibilities," which depends in large part on how independent third parties (*i.e.*, the banks) determine to act and exercise judgment, does not establish Article III standing. *See Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 410-414 (2013) (respondents lacked standing where, as here, alleged injury required a "highly attenuated chain of possibilities," predicated in part on assumptions as to how independent, third-party decisionmakers would exercise their discretion in

[8] Even where fraudulent charges *have* been alleged (which they have not here), courts have found such charges—without more—are insufficient to confer Article III standing unless Plaintiffs have also alleged those charged were not reimbursed. *E.g.*, *Ables v. Brooks Bros. Grp.*, No. CV 17-4309-DMG (EX), 2018 WL 8806667, at *5 (C.D. Cal. June 7, 2018).

applying the law). This case requires a similar result to *Clapper*, and Plaintiffs' CAC should be dismissed for their failure to articulate any concrete, actual injury.

"Diminished Value of Rights to Protection of Data." Plaintiffs' allegation that they were somehow harmed by the purported "diminished value of their rights to protection of their banking data" (CAC ¶¶ 225, 227) is too conclusory and vague to support standing under Article III. *See Whitmore*, 495 U.S. at 155. Plaintiffs do not allege any facts to show what valuable "rights" or "protections" were diminished. This hypothetical diminution of unspecified rights and protections is legally insufficient to establish injury in fact under Article III. However, even if Plaintiffs had adequately alleged a concrete diminution in value (due to allegedly insufficient data security protections), which they clearly have not, such bare allegations would be insufficient to show harm under Article III. *See*, *e.g.*, *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955, 973 & n.5 (N.D. Cal. 2015), *aff'd*, 717 F. App'x 720 (9th Cir. 2017) (finding transmitting information to data centers with allegedly insufficient security, without evidence of a breach, insufficient for Article III standing).

"Loss of Control Over Valuable Property." It is not clear what harm Plaintiffs actually claim from a supposed "loss of control" over valuable property (CAC ¶¶ 228-231), but in any event, such alleged harm certainly is not "concrete," "distinct and palpable." *Whitmore*, 495 U.S. at 155. "[I]njury-in-fact in this context requires more than an allegation that a defendant profited from a plaintiff's personal … information. Rather, a plaintiff must allege how the defendant's use of the information deprived the plaintiff of the information's economic value." *In re Google, Inc. Privacy Policy Litig.*, No. C-12-01382-PSG, 2013 WL 6248499, at *5 (N.D. Cal. Dec. 3, 2013). Plaintiffs notably do not do so, nor do they allege that they "lost dollars of [their] own." *Id*. Thus, their supposed "harm" is insufficient to confer standing under Article III.

"Increased Risk of Identity Theft and Fraud." Plaintiffs claim that Plaid's alleged removal of "sensitive banking data from the secure banking environment," by itself, has somehow increased their risk of identity theft and fraud. CAC ¶¶ 232-235. But "threatened injury must be *certainly impending* to constitute injury in fact, and … [a]llegations of *possible* future injury are not sufficient." *Clapper*, 568 U.S. at 409 (internal quotations omitted, emphasis in original); *see also Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (requiring "a credible threat of real

and immediate harm"). Indeed, courts routinely reject arguments similar to Plaintiffs' allegations. For example, in *Katz*, the court rejected the plaintiff's allegation that she had suffered injury in fact as a result of an increased risk that someone *might* access her data due to purportedly inadequate protections. *Katz v. Pershing LLC*, 672 F.3d 64, 70 (1st Cir. 2012). The court held the alleged increased risk, "unanchored to any actual incident of data breach," was insufficient to "satisfy Article III's requirement of actual or impending injury," and emphasized that the plaintiff's failure to "identify any incident in which her data has ever been accessed by an unauthorized person" was a "fatal" omission. *Id*. at 80; *see also Low v. LinkedIn Corp.*, No. 11-cv-01468-LHK, 2011 WL 5509848, at *5-6 (N.D. Cal. Nov. 11, 2011) (plaintiff failed to establish "credible threat" in absence of "publication or theft" of personally identifying information). Plaintiffs' bare allegation of "increased risk"—unanchored to any actual incident of data breach—is thus insufficient to satisfy Article III.[9]

Plaintiffs' lack of any impending injury or credible threat is further underscored by the fact that many years—six and a half for several Plaintiffs—have elapsed since most Plaintiffs started using the apps referenced in the CAC, and they do not allege the occurrence of any incident, let alone an identity theft or security breach, during this significant passage of time. *See*, *e.g.*, CAC ¶¶ 150; 178. Courts recognize that the absence of any theft during the time following a security incident weighs heavily *against* a finding of "immediate, credible risk of harm." *See*, *e.g.*, *Fernandez v. Leidos, Inc*., 127 F. Supp. 3d 1078, 1087 (E.D. Cal. 2015) (four years after incident without identity theft showed risk was not imminent); *In re Sci. Applications Int'l Corp. ("SAIC") Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 34 (D.D.C. 2014) (no incident, thirty-four months post-breach, showed no imminent harm). This reasoning applies with even greater force here, where significant time has passed without any alleged incident, let alone theft.

[9] Even where (unlike here) there *has already been an alleged data breach*, courts have still found no "certainly impending harm" under Article III, where there is no real and immediate risk of identity theft. *See*, *e.g.*, *In re Uber Techs., Inc., Data Sec. Breach Litig*., No. CV 18-2970 GJSx, 2019 WL 6522843, at *4-5 (C.D. Cal. Aug. 19, 2019) (holding data breach failed to create a certainly impending risk of identity theft); *Antman v. Uber Techs., Inc.*, No. 3:15-CV-01175-LB, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) (no "credible risk of identity theft that risks real, immediate injury" even after a data breach).

Finally, to the extent Plaintiffs try to assign value to the purported time and effort spent monitoring financial accounts due to some speculative increased "risk" (CAC ¶¶ 108, 118, 128, 138, 148, 157, 166, 176, 186, 197, 206), monitoring can only constitute injury in fact if the risk of immediate harm is "real and imminent," which it is not here, as set forth above. *See*, *e.g.*, *In re Uber Techs., Inc., Data Sec. Breach Litig.*, 2019 WL 6522843, at *5. Plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Clapper*, 568 U.S. at 416.

b. Plaintiffs fail to sufficiently plead any "Invasions of Privacy and Dignitary Violations."

"Dignitary Violations." Although Plaintiffs allege violation of their "dignitary rights" and "dignitary interests" (CAC ¶¶ 208-213), these phrases lack concrete meaning and do not constitute "injuries in fact" except in narrow circumstances not applicable here involving discrimination or defamation. *See*, *e.g.*, *Brintley v. Aeroquip Credit Union*, 936 F.3d 489, 493-94 (6th Cir. 2019) (dignitary harm may give rise to standing only where plaintiff is "personally subject to the challenged discrimination"). Outside of these circumstances, courts reject "dignitary injury" because "[a]llowing [a plaintiff's] claim to proceed based on dignitary harm alone would undermine the notion that 'standing *requires a concrete injury* even in the context of a statutory violation.'" *Carroll v. Farmers & Miners Bank*, No. 2:17CV00049, 2018 WL 1659481, at *2 (W.D. Va. Apr. 5, 2018) (quoting *Spokeo*, 136 S. Ct. at 1549) (emphasis in original).

"Invasions of Privacy." Plaintiffs claim invasion of privacy as a result of alleged "unauthorized parties accessing, storing, selling, and using [their] most private financial information and intruding upon [their] private affairs and concerns." CAC ¶¶ 108, 118, 128, 138, 148, 157, 166, 176, 186, 197, 206; *see also id.* ¶¶ 208, 209. But Plaintiffs do not even allege they linked their financial accounts to their chosen apps through Plaid, let alone facts showing unauthorized access or intrusion by Plaid or that Plaid caused them any harm. While some courts have found that mere invasion of privacy, without a showing of additional harm, can be sufficient for Article III purposes (*see*, *e.g.*, *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020)), the invasion of

privacy alleged still must be "real" and "actual," which it is not here. *Id*. at 598 ("A concrete injury is one that is real and not abstract."); *Whitmore*, 495 U.S. at 155; *Spokeo*, 136 S. Ct. at 1548.

In *In re Facebook, Inc. Internet Tracking Litigation*, the court found that the plaintiffs' alleged "invasion of privacy" constituted a "real" or "actual" harm based on specific factual circumstances not present in this case: (1) the plaintiffs lacked any "meaningful opportunity to control or prevent the unauthorized exploration of their private lives," and (2) the plaintiffs did not consent to the collection of information because that information was not only undisclosed in Facebook's Data Use Policy, but Facebook affirmatively represented it would not collect such information. 956 F.3d at 598-99. Here, there is no "real" or "actual" harm because Plaintiffs (1) have a meaningful opportunity to control or prevent any "exploration" of their alleged "private lives" (Plaintiffs could link their financial accounts without Plaid, or could request to delete their data or disconnect their accounts at any time); and (2) do not plausibly allege Plaid collected data in a manner not disclosed in its Privacy Policy (*supra*, at 4-5), let alone that Plaid affirmatively represented that it would not collect data that it then proceeded to collect. *Id*.

(1) Meaningful opportunity to control or prevent "exploration": Plaintiffs concede they *intended* to provide their chosen apps with access to their data for the purpose of sending and receiving payments (CAC ¶¶ 100, 111, 121, 130, 140, 150, 159, 168, 178, 188, 199), thus directly contradicting their claim that there was unauthorized access. In any event, every single Plaintiff had the opportunity to control or prevent the purported "unauthorized" invasion; as discussed above, they could connect without Plaid, or disconnect their accounts or request to delete their data at any time. Yet, not a single Plaintiff alleges any attempt to disconnect their accounts or delete their data from their chosen apps. Plaintiffs' failure to allege any attempt to stop their alleged "harm" makes any claim of actual injury implausible. *See Whitmore*, 495 U.S. at 155; *Spokeo*, 136 S. Ct. at 1548.

(2) Disclosure of data collected in Privacy Policy: Plaintiffs' "invasion of privacy" allegations are also undercut by the express disclosures in Plaid's Privacy Policy, which address exactly how Plaid accesses, collects and uses data. *Supra*, at 4-5.

In cases like this one—where no concrete harm is alleged—courts dismiss invasion of privacy claims for lack of standing. *See*, *e.g.*, *Cahen*, 147 F. Supp. 3d at 971-72 (dismissing claim under

Article III because plaintiffs had not alleged "concrete harm from the alleged collection and tracking of their personal information sufficient to create injury in fact"; there was no "theft, malicious breach, or widespread accidental publication of sensitive personally identifying information").[10]

2. Plaintiffs do not allege facts showing Plaid caused them any injury.

Article III requires "a causal connection between the injury and the conduct complained of—the injury has to be fairly … trace[able] to the challenged action of the defendant." *Lujan*, 504 U.S. at 560 (internal quotations omitted). While Plaintiffs allege they "signed up to use" various fintech apps (*e.g.*, CAC ¶ 100), the act of signing up—or even linking a financial account to an app—does not require Plaid's involvement. Instead, as demonstrated with the Venmo example referenced in the CAC, Plaid plays a role only if and when an end user links an account to an app *through Plaid* rather than by some other means (*e.g.*, through a company other than Plaid or through an entirely different linking method). *Supra*, at 6-7. Here, not a single Plaintiff alleges linking an account to an app through Plaid—let alone facts to show Plaid *caused* any harm as a result of any linkage. Plaintiffs' claims fail because they do not allege facts to show the requisite causal nexus between their alleged injury and any purported conduct by Plaid. *See*, *e.g.*, *In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *7 (N.D. Cal. Sept. 20, 2011) (no causation where plaintiffs did not "provide specific allegations with respect to the causal connection between the exact harm alleged (whatever it is) and each Defendants' conduct or role in that harm.").

3. Plaintiffs do not allege how their speculative claims are redressable.

Plaintiffs fail to plead how their illusory, speculative injuries (which are in and of themselves insufficient for Article III standing) are "likely to be redressed by a favorable decision." *See Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 38, 41 (1976); *see also Spokeo*, 136 S. Ct. at 1547. Indeed, any such "relief" would only provide "psychic satisfaction," which "is not an acceptable Article III

[10] Even if Plaintiffs' invasion of privacy claim was sufficient under Article III (it is not), this "harm" would only be "sufficient to confer standing for those claims on which the injury bears—intrusion upon seclusion and public disclosure of private facts." *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1058 (N.D. Cal. 2014) (dismissing Plaintiffs' common law claims, except invasion of privacy, on standing grounds). Plaintiffs would still lack standing to pursue all other claims. Further, their common law and constitutional privacy claims would still be legally insufficient and subject to dismissal as discussed herein. *See*, *infra*, at Section IV. D. 5.

remedy." *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 107 (1998) ("[r]elief that does not remedy the injury suffered cannot bootstrap a plaintiff into federal court").

B. Most of Plaintiffs' claims are barred by the statutes of limitation.

Even if Plaintiffs had connected their financial accounts through Plaid when they signed up with their chosen apps, the vast majority of Plaintiffs' claims are barred as a matter of law by the applicable statutes of limitation.

1. The statutes of limitation accrued at the time of the alleged injuries, the majority of which occurred over four years prior to filing the CAC.

Even under the longest statute applicable to Plaintiffs' claims (four years),[11] most of the Plaintiffs' claims expired well before the initial complaint or the CAC were filed (in May 2020 and August 2020). A cause of action accrues "when the cause of action is complete with all of its elements." *Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal. 4th 797, 806 (2005). For the purpose of this claim, since Plaintiffs do not allege linking through Plaid at all, or even *when* they connected their financial accounts, that occurred when each Plaintiff signed up to use the apps described in the CAC, as depicted in the chart in the Dettmer Decl. ¶ 7. In sum, based on the allegations in the CAC:

- All claims by Plaintiffs Curtis (April 2015, CAC ¶ 121), Mitchell (Aug. 2015, *id*. ¶ 140), Mullen (March 2014, *id*. ¶ 150), Sacks (June 2014, *id*. ¶ 159), and Yeomelakis (March 2014, *id*. ¶ 199) are time-barred because they accrued in 2015 or earlier when they allegedly signed up for the apps, and thus expired before the filing of the plaintiffs' respective complaints;
- All of Plaintiffs Schoeneman's and Evans' claims are time-barred except their UCL claims (as Mr. Schoeneman allegedly signed up for Venmo in July 2016 (*id*. ¶ 168) and Mr. Evans allegedly signed up in the summer of 2016 (*id*. ¶ 130) and the UCL's statute of limitations is four years);
- All of Mr. Umali's claims are time-barred except his UCL claim in connection with his use of Coinbase (as he allegedly signed up for Coinbase in 2017 (*id*. ¶ 189) and the UCL's statute of limitations is four years); and
- No claims by Plaintiffs Anderson, Cottle, and Sotelo are time-barred, based on the current allegations (but should be dismissed for other reasons set forth herein).[12]

[11] Common law invasion of privacy, Cal. Code. Civ. P. § 335.1 (two years); CFAA, 18 U.S.C. § 1030(g) (two years); SCA, 18 U.S.C. § 2707(f) (two years); declaratory judgment and injunctive relief, *Maguire v. Hibernia Sav. & Loan Soc*., 23 Cal. 2d 719, 734 (1944) (same statute of limitations as applies to the underlying request for declaratory relief); unjust enrichment, *Creditors Collection Serv. v. Castaldi*, 38 Cal. App. 4th 1039, 1044 (1995) (citing Cal. Civ. Code § 338(d)) (three years); UCL, Cal. Bus. & Prof. Code § 17208 (four years); Article I, Section I of the Cal. Const., Cal. Civ. Code § 335.1 (two years); CAPA, Cal. Civ. Code § 338(d) (three years); Deceit, Cal. Civ. Code §§ 1709, 338(d) (three years); CDAFA, Cal. Penal Code § 502(e)(5) (three years).

[12] Plaid concedes that certain claims are not time-barred for the purpose of this motion only, and reserves its rights to challenge all claims on the basis of the relevant statutes of limitation at a later date. Discovery (if necessary) would likely demonstrate that these claims are also time-barred.

2. The limitation periods should not be tolled.

Plaintiffs claim the discovery rule, fraudulent concealment, and equitable estoppel tolled the applicable statutes of limitation. CAC ¶¶ 239-243. Plaintiffs must plead facts to support these defenses (*McKelvey v. Boeing N. Am., Inc.*, 74 Cal. App. 4th 151, 160 (1999)), yet they fail to do so.

First, under the discovery rule, even if Plaintiffs had alleged connecting through Plaid, they would have "kn[own] or ha[d] reason to know of the injury" upon signing up for the fintech apps and linking their accounts, when Plaid's Privacy Policy was available to them. *See Mangum v. Action Collection Serv., Inc.*, 575 F.3d 935, 940 (9th Cir. 2009); *Kline v. Turner*, 87 Cal. App. 4th 1369 (2001). A plaintiff does not need to know specific facts necessary to establish the claim; facts that can reasonably be discovered are sufficient. *Jolly v. Eli Lilly & Co.*, 44 Cal. 3d 1103, 1111 (1988).

Second, for fraudulent concealment, Plaintiffs must show Plaid affirmatively misled them, and that they had no "actual or constructive knowledge" despite "diligence in trying to uncover those facts." *See Hexcel Corp. v. Ineos Polymer, Inc.*, 681 F.3d 1055, 1060 (9th Cir. 2012). But Plaid's Privacy Policy discloses the data Plaid collects, and how it is used, foreclosing any argument that Plaid "affirmatively misled" Plaintiffs and foreclosing any fraudulent concealment defense. *Id.*

Finally, courts only apply equitable estoppel where a "defendant has affirmatively sought to mislead the charging party," and actually and reasonably induced the plaintiffs into waiting to sue. *Diaz v. Safeway Inc.*, No. C-07-01902 RMW, 2007 WL 2793367, at *5 (N.D. Cal. Sept. 26, 2007). Plaintiffs do not allege Plaid induced them to postpone suit.

In sum, most of the Plaintiffs' claims are untimely and should be dismissed with prejudice.

C. Plaintiffs have an adequate remedy at law, and thus their equitable claims are barred.

A claim for equitable relief is proper only where "the remedies available at law are inadequate." *Franklin v. Gwinnett Cty. Pub. Sch.*, 503 U.S. 60, 75-76 (1992). Where, as here, a legal remedy, such as monetary damages, is available,[13] courts routinely dismiss equitable claims and remedies. *See*, *e.g.*, *Sonner v. Premier Nutrition Corp.*, -- F.3d --, 2020 WL 4882896, at *7 (9th Cir.

[13] *Mullins v. Premier Nutrition Corp.*, No. 13-CV-01271-RS, 2018 WL 510139, at *2 (N.D. Cal. Jan. 23, 2018) ("[T]he relevant test is whether an adequate damages remedy is available, not whether the plaintiff elects to pursue it, or whether she will be successful in that pursuit."); *see also Schroeder v. United States*, 569 F.3d 956, 963 (9th Cir. 2009).

June 17, 2020) (explaining a plaintiff "must establish that she lacks an adequate remedy at law before securing equitable restitution for past harm under the UCL and CLRA"); *Philips v. Ford Motor Co.*, 726 F. App'x 608, 609 (9th Cir. 2018) (affirming dismissal of injunctive relief sought under the UCL because plaintiffs "were required to plead the inadequacy of their legal remedies").

Here, a legal remedy is not only available to Plaintiffs, but they actually seek damages that would compensate them for all harms they supposedly suffered (though those harms are legally insufficient). Plaintiffs do not claim such damages are inadequate. Because Plaintiffs have (and are pursuing) available remedies at law, their equitable claims and remedies—specifically, their UCL and unjust enrichment claims and all requests for disgorgement, restitution, injunctive and declaratory relief—must be dismissed. *See*, *e.g.*, *Sonner*, 2020 WL 4882896, at *7; *Diaz*, 2007 WL 2793367, at *5; *Zapata Fonseca v. Goya Foods Inc.*, No. 16-CV-02559-LHK, 2016 WL 4698942, at *7 (N.D. Cal. Sept. 8, 2016) (dismissing UCL, unjust enrichment, and other equitable claims); *Bird v. First Alert, Inc.*, No. C-14-3585-PJH, 2014 WL 7248734, at *5-6 (N.D. Cal. Dec. 19, 2014) (dismissing UCL claim because plaintiff "ha[d] an adequate remedy at law in her claim for damages under the" Consumers Legal Remedies Act); *Durkee v. Ford Motor Co.*, No. C 14-0617 PJH, 2014 WL 4352184, at *3 (N.D. Cal. Sept. 2, 2014) (dismissing request for injunctive relief because "[a] plaintiff seeking equitable relief must establish there is no adequate remedy at law available."); *Archer W. Contractors, LLC v. Int'l Fid. Ins. Co.*, No. 16-CV-1494 JLS (BGS), 2017 WL 4286970, at *7-8 (S.D. Cal. Sept. 27, 2017) (dismissing declaratory relief claim because damages claim provided adequate remedy at law); *Mullins*, 2018 WL 510139, at *4 (dismissing equitable restitution and disgorgement claims where plaintiff had adequate remedy at law).

Because the existence of adequate legal remedies is not curable, Plaintiffs' equitable "claims" (UCL, Unjust Enrichment, Declaratory and Injunctive Relief) should be dismissed ***with prejudice***. *See*, *e.g.*, *Loo v. Toyota Motor Sales, USA, Inc.*, No. 19-00750, 2019 WL 7753448, at *13-14 (C.D. Cal. Dec. 20, 2019) (dismissing UCL claim with prejudice that, as Plaintiffs' claim does here, relied on the "same factual predicates" as the legal claims).

D. The CAC fails to state plausible claims under Rule 12(b)(6), and should be dismissed.

Plaintiffs predicate their entire CAC on Plaid's alleged failure to disclose how it collects, uses, and shares data. *E.g.*, CAC ¶¶ 4, 37, 66, 70, 74(a). Specifically, Plaintiffs allege ten "facts" related to data collection, use, and sharing that "Plaid's privacy policy [allegedly] fails to disclose" (CAC ¶ 74(h)). But as demonstrated by the chart on pages 4-5, *supra*, each of these supposed omissions is not an omission at all, but instead contradicted by an express disclosure contained in the Privacy Policy (save for the tenth point, which just restates Plaintiffs' (incorrect) argument that Plaid destroys "valuable protections" provided by banks in the event of some hypothetical data breach). Where, as here, a document referenced in the complaint (*i.e.*, the Privacy Policy) directly undermines Plaintiffs' allegations, those allegations should be disregarded. *See Lazy Y Ranch Ltd. v. Behrens*, 546 F.3d 580, 588 (9th Cir. 2008) (the court "need not accept as true allegations contradicting documents that are referenced in the complaint or that are properly subject to judicial notice"); *Daniels-Hall v. Nat'l Educ. Ass'n*, 629 F.3d 992, 998 (9th Cir. 2010) (same). And without these allegations—which are the backbone of the CAC—all of Plaintiffs' claims necessarily fail. *See*, *e.g.*, *TBG Ins. Servs. Corp. v. Superior Ct.*, 96 Cal. App. 4th 443, 452 (2002) (no reasonable expectation of privacy in light of privacy policy); *Lewis v. Google LLC*, No. 20-CV-00085-SK, 2020 WL 2745253, at *14 (N.D. Cal. May 20, 2020) (no deceit where the "purportedly omitted fact is disclosed"). Simply put, Plaintiffs' claims are not plausible as a matter of law and should be dismissed with prejudice for this and each of the reasons discussed below.[14]

[14] Plaintiffs' conclusory claim that they did not consent to Plaid's Privacy Policy is not plausible and should be disregarded. Every named Plaintiff allegedly used Venmo, and Plaintiffs admit the Venmo Link pane contains a consent flow. *Id.* ¶¶ 67, 72. This is consistent with similar consent flows across the industry, which have been found to create valid and binding agreements between the parties. *See*, *e.g.*, *Peter v. DoorDash, Inc.*, No. 19-CV-06098-JST, 2020 WL 1967568, at *4 (N.D. Cal. Apr. 23, 2020) (noting "numerous cases in which courts have enforced agreements with substantially similar forms of notice" despite plaintiffs' claims of an "unreasonably small[,]" "gray font on a lighter-shade of gray background[,]" "not underlined to indicate a hyperlink"); *Meyer v. Uber Techs., Inc.*, 868 F.3d 66, 78 (2d Cir. 2017) (holding small font provided sufficient contractual notice). And the claim that "[s]ome apps, such as Square's Cash App … provide no disclosures whatsoever" is belied by those apps' terms and/or privacy policies. Indeed, Cash App's terms of service state: "[i]f you choose to link your Eligible Bank Account to your Cash App … you acknowledge your personal and financial information is being provided to Plaid Inc., [and] that your personal and financial information will be collected, processed, transferred, or stored in accordance with Plaid Inc.'s Privacy Policy[.]" Ex. C at 10. Coinbase's Privacy Policy also tells end users that it "may use Plaid" to connect and verify accounts and confirm account balances "prior to approving a

1. The legal standard applicable to motions to dismiss under Rule 12(b)(6).

To survive a motion to dismiss for failure to state a claim under Rule 12(b)(6), a complaint must state "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007); *see also Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A "plaintiff's obligation to provide the 'grounds' of his 'entitlement to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555 (citations omitted). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice … While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations." *Iqbal*, 556 U.S. at 678-80; *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004) ("[C]onclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss.").

2. Plaintiffs plead no plausible claim under California's Unfair Competition Law.

a. Plaintiffs fail to plausibly allege the required economic harm.

In addition to the reasons set forth in Section IV. C, *supra*, Plaintiffs' UCL claim fails for the additional reason that Plaintiffs have not pled, and cannot plead, that they lost money or property. Individuals may bring a UCL action only if they have "suffered injury in fact and ha[ve] lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204; *Birdsong v. Apple, Inc.*, 590 F.3d 955, 959 (9th Cir. 2009); *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310, 322-24 (2011). It is well settled that personal information does not constitute "lost money or property" under the UCL. *Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014) (misappropriation of private messages not lost "money and property"); *Archer v. United Rentals, Inc.*, 195 Cal. App. 4th 807, 816 (2011) (unlawful PII collection and recordation not lost money or property). As Plaintiffs have not alleged they lost money or property, their UCL claim fails.

transaction"; states "[i]nformation shared with Plaid is treated by Plaid in accordance with its Privacy Policy," and links to that policy. Ex. D at 7. And Venmo's Privacy Policy discloses it may share information with "third parties with your consent or at your direction to do so, including if you authorize an account connection with a third-party account or platform[.]" Ex. B at 6. Thus, end users who use these apps are notified that their information can be shared with a third party like Plaid.

b. Plaintiffs allege no unlawful, unfair, or fraudulent business practice.

The UCL prohibits business practices that are (1) unlawful, (2) unfair, or (3) fraudulent. Cal. Bus. & Prof. Code § 17200. Plaintiffs fail to state a claim under any of these three prongs.[15]

Plaintiffs do not adequately allege any "unlawful" business practice. Plaintiffs' claim under the UCL's "unlawful" prong is based on (1) alleged statutory violations underlying Plaintiffs' other causes of action, and (2) other statutes the CAC references but that are not stand-alone causes of action (Cal. Fin. Code § 4051, *et seq*. (CalFIPA); 16 C.F.R. Part 313 (GLBA); 12 C.F.R. Part 1016 (GLBA); and Cal. Bus. & Prof. Code § 22575, *et seq*. (CalOPPA)). With respect to the first category, Plaintiffs fail to allege facts sufficient to show Plaid violated the underlying laws as discussed herein, and their UCL claim fails along with those claims. *See*, *e.g.*, *Avila v. Countrywide Home Loans*, No. 10-CV-05485-LHK, 2010 WL 5071714, at *6 (N.D. Cal. Dec. 7, 2010) (dismissing UCL claim premised on violation of underlying law for which plaintiff failed to state claim).

With respect to the second category, Plaintiffs' attempt to allege a UCL violation based on GLBA, CalFIPA, and CalOPPA fares no better. GLBA and CalFIPA provide exclusive enforcement authority to the government—not private plaintiffs. 15 U.S.C. § 6805(a) (GLBA exclusively enforced by CFPB, FTC, federal regulators and state insurance authorities); Cal. Fin. Code § 4057(e) (CalFIPA exclusively enforced by California AG or functional regulator). Because these statutes preclude a private right of action, they cannot support a UCL claim. *See Zhang v. Super. Ct.*, 57 Cal. 4th 364, 384 (2013) (holding when private actions are barred, "a litigant may not rely on the proscriptions of [that statute] as the basis for a UCL claim.").[16] Nor can CalOPPA serve as the basis

[15] Plaid reserves all arguments related to Plaintiffs' claim that California law applies to "the claims of Plaintiffs and the Nationwide Class members" (CAC ¶ 236), and does not concede that all named Plaintiffs and the putative nationwide class can invoke California's UCL, invasion of privacy, and unjust enrichment laws. *See Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 589-94 (9th Cir. 2012) (finding "each class member's consumer protection claim should be governed by the consumer protection laws of the jurisdiction in which the transaction took place"); *Romero v. Flowers Bakeries, LLC*, No. 14-cv-05189-BLF, 2015 WL 2125004, at *9 n.3 (N.D. Cal. May 6, 2015) (it was "unclear which states' laws should apply" to fraud and unjust enrichment claims on behalf of nationwide class, and "other courts confronting the issues have noted differences among the unjust enrichment laws of different states").

[16] Plaintiffs also rely on inapplicable sections of the GLBA and CalFIPA, failing to acknowledge exemptions of these statutes' requirements where a financial institution shares personal information in connection with a consumer's request. Cal. Fin. Code § 4056(b)(1); 16 C.F.R. § 313.14(a), (b).

for Plaintiffs' UCL claim because Plaintiffs do not allege they purchased or leased anything from Plaid, a requirement to constitute "consumers" under CalOPPA. *See* Cal. Bus. & Prof. Code § 22577(d).[17] For these reasons, Plaintiffs' UCL "unlawful" claim fails.

Plaintiffs do not adequately allege any "unfair" business practice. Although courts are divided as to what constitutes an "unfair" activity under the UCL, Plaintiffs do not plead facts that demonstrate "unfair" conduct under any definition. While their CAC is replete with conclusory rhetoric, Plaintiffs have pled no ***facts*** plausibly suggesting Plaid's acts, omissions, or conduct "offend[] an established public policy [or that they are] immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." *McDonald v. Coldwell Banker*, 543 F.3d 498, 506 (9th Cir. 2008) (internal quotation marks and citation omitted). Plaintiffs do not allege any details or facts indicating how Plaid's conduct is unfair, other than the conclusory allegations contained in CAC ¶¶ 331-333, tying alleged "important public interests" to the same statutory and common law claims analyzed throughout this motion. The Court should dismiss the UCL "unfairness" claim for the same reasons those statutory and common law claims fail, as discussed herein. *See Smith & Hawken, Ltd. v. Gardendance, Inc.*, No. C04–1664 SBA, 2004 WL 2496163, at *5 (N.D. Cal. Nov. 5, 2004) (dismissing UCL claim for failure to allege conduct was "unfair" under any test).

Plaintiffs do not adequately allege any "fraudulent" business practice. Plaintiffs cannot state a claim under the UCL's "fraud" prong because they fail to satisfy the minimal pleading requirements of Rule 8, much less the particularity requirements under Rule 9(b). *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009) (noting heightened pleading standard of Rule 9(b) applies to UCL claims that are "grounded in fraud"); *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003) ("Averments of fraud must be accompanied by the 'who, what, when, where,

[17] Furthermore, CalOPPA only covers "information from a consumer residing in California," foreclosing the statute for many Plaintiffs. *See id*. § 22577(c). Additionally, in compliance with CalOPPA's rules governing the content and display of privacy policies by companies collecting personally identifiable information about California consumers (Cal. Bus. & Prof. Code § 22575 *et seq.*), Plaid's Privacy Policy discloses "the categories of personally identifiable information" it collects and "the categories of third-party persons or entities with whom [it] may share" that information. *Supra* at 4-5. "Online services" like Plaid's (CAC ¶ 97) can make their privacy policies available by any "reasonably accessible means." Cal. Bus. & Prof. Code § 22577(b)(5). "Online services" do not have the same requirements as websites. Cal. Bus. & Prof. Code § 22575(b). Yet Plaintiffs cite the wrong standard (the one for websites), and do not mention the actual applicable standard (for "online services") or allege that Plaid violated it.

and how' of the misconduct charged."). Plaintiffs have not alleged the "who, what, when, where, and how" of their claim (*infra*, at 35-36), let alone that they actually relied on any purported misrepresentation or omission by Plaid, which is fatal to their UCL "fraud" claim. *See In re Tobacco II Cases*, 46 Cal. 4th 298, 326 (2009).

Plaintiffs cannot obtain restitution or disgorgement under the UCL. Finally, Plaintiffs claim they are entitled to disgorgement under the UCL. CAC ¶ 347. However, a court may only order restitution "as may be necessary to *restore* to any person in interest any money or property … acquired by means of such unfair competition." Cal. Bus. & Prof. Code § 17203 (emphasis added). It is well-established that a party is barred from nonrestitutionary disgorgement "under the UCL where these profits are neither money taken from a plaintiff nor funds in which the plaintiff has an ownership interest." *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1140 (2003); *see also Madrid v. Perot Sys. Corp*., 130 Cal. App. 4th 440, 460 (2005) (nonrestitutionary disgorgement unavailable under UCL). Plaintiffs do not allege Plaid received any money or property from them to return. Even assuming Plaintiffs linked their bank accounts to fintech apps using Plaid (which the CAC fails to allege), the CAC nowhere alleges any facts indicating Plaintiffs gave any money or property to Plaid. Nor could they—Plaid does not charge end users for its services. Accordingly, the Court should dismiss the request for restitution and disgorgement under the UCL.

3. Plaintiffs fail to plead plausible claims under the CFAA and the CDAFA.

a. The CFAA and CDAFA are anti-hacking statutes that do not apply here.

Plaintiffs allege violations of six subsections of the CFAA (Computer Fraud and Abuse Act) (18 U.S.C. § 1030(a)(2), (4), (5)(A)-(C), (6)), and seven subsections of its California equivalent, the CDAFA[18] (Comprehensive Computer Data Access and Fraud Act) (Cal. Penal Code § 502(c)(1)-(4), (6)-(8)). These narrow statutes are intended "to punish hacking—the circumvention of technological access barriers"—and should not be transformed "from an anti-hacking statute into an expansive misappropriation statute." *United States v. Nosal*, 676 F.3d 854, 857, 857 (9th Cir. 2012) (discussing CFAA); *see also Custom Packaging Supply, Inc. v. Phillips*, No. 2:15-CV-04584-ODW-AGR, 2015

[18] Plaintiffs only bring their claims under the California Constitution, Anti-Phishing Act, Cal. Civ. Code §§ 1709-1710 (deceit), and CDAFA on behalf of the putative California class. CAC ¶¶ 339, 350, 357, 365.

WL 8334793, at *3 (C.D. Cal. Dec. 7, 2015) (the CDAFA "is an anti-hacking statute intended to prohibit the unauthorized use of any computer system for improper or illegitimate purpose."). Plaintiffs do not and cannot allege hacking or any facts suggestive of hacking, and these statutes thus do not apply. However, even assuming Plaintiffs could overcome this fatal hurdle, their claims fail for the additional reasons below.

b. Plaintiffs have no standing to bring civil claims under these statutes.

The CFAA and CDAFA are criminal statutes and provide for civil liability only in narrow circumstances not present here. A private right of action exists under the CFAA only for a person who has suffered actual "economic damages" aggregating at least $5,000 during any 1-year period caused by an alleged computer fraud. 18 U.S.C. §§ 1030(g), 1030(c)(4)(A)(i)(I); *see also Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 313 F. Supp. 3d 1056, 1069 (N.D. Cal. 2018).[19] Although the CDAFA does not include an explicit monetary threshold, it requires pleading facts to show "damage or loss by reason of a violation." Cal. Penal Code § 502(e)(1); *see also Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1219 (N.D. Cal. 2014) (dismissing case where plaintiffs failed to adequately allege "Plaintiffs have suffered any tangible harm from the alleged Section 502 violations"). Here, Plaintiffs have failed to plead *any* "tangible harm," let alone an economic loss of at least $5,000, caused by any purported hacking. Their conclusory recitations of the statutes (*see*, *e.g.*, CAC ¶ 297; CAC ¶ 378) are legally insufficient. *See*, *e.g.*, *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1064 (N.D. Cal. 2012) (dismissing CFAA claims of economic loss for personal information collection); *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1090 (N.D. Cal. 2018) (dismissing CDAFA claim because "boilerplate allegations do not survive Rule 8").

Further, civil standing under the CDAFA §§ 502(c)(3), (6), and (7) only exists for the *owner* of the computer services or computer attacked and damaged. Cal. Penal Code § 502(e)(1); *Gonzales*, 305 F. Supp. 3d at 1090 (dismissing CDAFA claim for failure to allege access to "*Plaintiff's*

[19] A civil action can only be brought if the conduct involves one of the first five factors set forth in § 1030(c)(4)(A)(i). 18 U.S.C. § 1030(g). Plaintiffs only allege violation of the first subsection (*id.* § 1030(c)(4)(A)(i)(I)) (CAC ¶¶ 270-298), which requires loss "aggregating at least $5,000 in value." Additionally, "[d]amages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to 'economic damages.'" *Id.* § 1030(g). Thus Plaintiffs' corresponding claim for "injunctive and other equitable relief" (CAC ¶ 297) must be dismissed.

computer, computer system, etc."). Plaintiffs' allegations under these sections are based on Plaid's access to their "financial institutions' computers" (CAC ¶¶ 369-374), not *their own.*[20] Thus, Plaintiffs' claims based on §§ 502(c)(3), (6), and (7) should be dismissed for this additional reason.

c. Plaintiffs plead no elements of a claim under the CFAA or the CDAFA.

Plaintiffs' claims also fail because they do not plausibly allege conduct that violates the CFAA or CDAFA. Plaintiffs largely "parrot[] the language of the subsections" of these statutes, making conclusory claims that are insufficient under Rule 8.[21] *See Gonzales, Inc.*, 305 F. Supp. 3d at 1090 (N.D. Cal. 2018) (dismissing conclusory hacking claims). Plaintiffs' CFAA and CDAFA claims fail for many independent reasons, summarized in the following charts and discussed below.

CFAA

Section (18 U.S.C.)	Requisite Elements Of The Statute	Elements Plaintiffs Fail To Plausibly Allege
1030(a)(2)	"intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— (A) information contained in a financial record of a financial institution [or] … (C) information from any protected computer."	• No "economic damages" "aggregating at least $5,000" • No unauthorized or exceeding authorized access
1030(a)(4)	"knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access"	• No "economic damages" "aggregating at least $5,000" • No unauthorized or exceeding authorized access • No intent to defraud
1030(a)(5)(A)	"knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage	• No "economic damages" "aggregating at least $5,000" • No unauthorized access • No damage to any computer or data • No intent

[20] Plaintiffs claim their "mobile devices" "constitute 'computers, computer systems, and/or computer networks'" under the CDAFA (CAC ¶ 368), but the only claim alleging access to their mobile devices is the claim under § 502(c)(8), which should be dismissed as described *infra*, at 28-29.

[21] While the plain language of the CFAA and the CDAFA precludes liability, to the extent the Court finds ambiguity in those statutes, the rule of lenity requires interpretation in Plaid's favor—if there are two reasonable interpretations of the statutes, they must not be expanded, but rather be interpreted narrowly. *See Crandon v. United States*, 494 U.S. 152, 158 (1990) (rule of lenity applies in civil contexts where "the governing standard [for civil liability] is set forth in a criminal statute"); *Oracle Am., Inc.*, 2014 WL 31344, at *6 (applying "the bias towards lenity required of statutes like the CFAA" to dismiss claim); *Facebook, Inc. v. Power Ventures, Inc.*, No. C 08-05780 JW, 2010 WL 3291750, at *10 (N.D. Cal. July 20, 2010) (applying the rule of lenity to CDAFA claims). This rule also applies to any ambiguities in the SCA and the Anti-Phishing Act.

Section (18 U.S.C.)	Requisite Elements Of The Statute	Elements Plaintiffs Fail To Plausibly Allege
	without authorization, to a protected computer"	• No virus or computer contaminate
1030(a)(5)(B)	"intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage"	• No "economic damages" "aggregating at least $5,000" • No unauthorized access • No damage to any computer or data • No reckless conduct
1030(a)(5)(C)	"intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss"	• No "economic damages" "aggregating at least $5,000" • No unauthorized access • No damage to any computer or data
1030(a)(6)	"knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization"	• No "economic damages" "aggregating at least $5,000" • No intent to defraud • No password trafficking

CDAFA

Section (Cal. Penal Code)	Requisite Elements Of The Statute	Elements Plaintiffs Fail To Plausibly Allege
502(c)(1)	"Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data."	• No "damage or loss" suffered by Plaintiffs • No access without permission • No damage to any computer or data
502(c)(2)	"Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network."	• No "damage or loss" suffered by Plaintiffs • No access without permission
502(c)(3)	"Knowingly and without permission uses or causes to be used computer services."	• No "damage or loss" suffered by Plaintiffs • No damage alleged to *Plaintiffs'* computers (as opposed to third-party computers) • No use without permission
502(c)(4)	"Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network."	• No "damage or loss" suffered by Plaintiffs • No access without permission • No damage to any computer or data

Section (Cal. Penal Code)	Requisite Elements Of The Statute	Elements Plaintiffs Fail To Plausibly Allege
502(c)(6)	"Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section."	• No "damage or loss" suffered by Plaintiffs • No damage alleged to *Plaintiffs'* computers (as opposed to third-party computers) • No password trafficking • No lack of permission
502(c)(7)	"Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."	• No "damage or loss" suffered by Plaintiffs • No damage alleged to *Plaintiffs'* computers (as opposed to third-party computers) • No access without permission
502(c)(8)	"Knowingly introduces any computer contaminant into any computer, computer system, or computer network."	• No "damage or loss" suffered by Plaintiffs • No access without permission • No virus or computer contaminate

Plaintiffs fail to plead facts to show Plaid accessed a computer or data without authorization. The CFAA makes it unlawful for a person to intentionally access a computer without authorization (*i.e.*, without any permission at all) or to exceed authorization in accessing a computer (*i.e.*, by accessing information the person is not entitled to access). 18 U.S.C. §§ 1030(a)(2), (4); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009).[22] The CDAFA makes it unlawful to access a computer, and in some instances, data, "without permission." Cal. Penal Code § 502(c)(1)-(4), (6)-(8).

Here, Plaintiffs do not plausibly allege Plaid accessed any computer or data without, or in excess of, authorization; in fact they concede just the opposite by alleging they wanted their chosen apps to be linked to their financial accounts. *See*, *e.g.*, CAC ¶¶ 100, 109; *In re Apple & ATTM Antitrust Litig.*, No. C07-05152 JW, 2010 WL 3521965, at *7 (N.D. Cal. July 8, 2010)[23] ("[v]oluntary installation runs counter to the … CFAA's requirement that the alleged act was

[22] Access that exceeds authorization relates to accessing information that the defendant was not entitled to access, not misusing information accessed. *Nosal*, 676 F.3d at 858-59 (9th Cir. 2012) (refusing to "expand [the CFAA's] scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer"); *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, No. 19-1235, 2020 WL 5406118, at *3 (6th Cir. Sept. 9, 2020) (holding CFAA's aim "is penalizing those who breach cyber barriers without permission, rather than policing those who misuse the data they are authorized to obtain.").

[23] *Vacated in part on other grounds sub nom. In re Apple & AT & TM Antitrust Litig.*, 826 F. Supp. 2d 1168 (N.D. Cal. 2011).

'without authorization' as well as the [CDAFA]'s requirement that the act was 'without permission'"). "Simply put, [one] cannot access a computer 'without authorization' if the gatekeeper has given them permission to use it." *AtPac, Inc. v. Aptitude Sols., Inc.*, 730 F. Supp. 2d 1174, 1180 (E.D. Cal. 2010). Because Plaintiffs chose to link their accounts (whether through Plaid or not)—and because Plaid's Privacy Policy lists the data Plaid can collect—Plaintiffs cannot plausibly plead that Plaid accessed any computer or data without or in excess of authorization.[24]

Plaintiffs fail to sufficiently plead "damage" under CFAA § 1030(a)(5) or CDAFA §§ 502(c)(1) and (4). Plaintiffs' claims under CFAA §§ 1030(a)(5)(A)-(C) fail for the additional reason that they have not plausibly alleged any conduct that intentionally or recklessly "cause[d] damage," defined under the statute as "any impairment to the integrity or availability of data, a program, a system, or information[.]" 18 U.S.C. § 1030(e)(8). This requirement is distinct from damage to *Plaintiffs*, and requires damage to *systems or data*. Plaintiffs claim Plaid "impaired the integrity" of their data and smartphones (CAC ¶¶ 285, 288, 291). But "simply download[ing] the data requested without leaving a trace" "[does] not impair the integrity or availability of" data or systems, and "is not 'damage' as defined by the statute." *Fidlar Techs. v. LPS Real Estate Data Sols., Inc.*, 810 F.3d 1075, 1084 (7th Cir. 2016); *see also*, *e.g.*, *NetApp, Inc. v. Nimble Storage, Inc.*, No. 5:13-CV-05058-LHKHRL, 2015 WL 400251, at *14 (N.D. Cal. Jan. 29, 2015) (copying information and transferring it to "a non-secure area or device" is not "damage" under the CFAA). Nor do Plaintiffs allege facts to show Plaid caused any "damage" intentionally or recklessly. *C.f. In re Apple & ATTM Antitrust Litig.*, 2010 WL 3521965, at *7 (finding lack of evidence "Apple acted with an intent to damage Plaintiffs' iPhones" fatal to CFAA claim).

Plaintiffs also allege no facts showing Plaid "add[ed], alter[ed], damage[d], delete[d], or destroy[ed] any data, computer software, or computer programs" as proscribed by § 502(c)(4), or that Plaid "alter[ed], damage[d], delete[d], destroy[ed], or otherwise use[d] any data, computer, computer system, or computer network" as required by § 502(c)(1). They only allege Plaid "damage[d] the

[24] Plaintiffs' allegation that notice of Plaid's Privacy Policy was insufficiently conspicuous, even if true (it is not), cannot form the basis for a claim under the CFAA or CDAFA. *See Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016) (no violation if defendant "reasonably could have thought" she had permission).

integrity" of their data (CAC ¶ 372), which is not "damage" recognized by these provisions of the CFAA. *See Ticketmaster L.L.C. v. Prestige Entm't W., Inc.*, 315 F. Supp. 3d 1147, 1175 & n.5 (C.D. Cal. 2018) (dismissing claims under subsections (c)(1) and (c)(4) for failure to allege damage, "narrowly construe[ing] 'otherwise uses' in section 502(c)(1) to refer to uses that involve data alteration, damage, deletion, and destruction").

Plaintiffs do not plead "intent to defraud" as required under CFAA §§ 1030(a)(4) and (a)(6). Intent to defraud under the CFAA "means that the defendant acted willfully and with specific intent to deceive or cheat, usually for the purpose of getting financial gain for himself or causing financial loss to another." *Fidlar*, 810 F.3d at 1079. Plaintiffs allege Plaid "acted with intent to defraud" because it intended to access and use Plaintiffs' data (CAC ¶¶ 280, 295), but they do not allege—nor can they, let alone with the specificity required by Rule 9(b)—that Plaid intended "to deceive or cheat." *Id*. To the contrary, Plaintiffs acknowledge that Plaid's *business* is to facilitate financial transactions via "bank 'linking' and verification." CAC ¶ 32.

Plaintiffs fail to allege password trafficking under CFAA § 1030(a)(6). Section 1030(a)(6) prohibits "knowingly and with intent to defraud traffic[king] in any password … or similar information through which a computer may be accessed without authorization," and defines "traffic" as "[to] transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." 18 U.S.C. §§ 1030(a)(6), 1029(e)(5). Plaintiffs allege Plaid violated § 1030(a)(6) by transferring access tokens to fintech apps. CAC ¶¶ 293-295. But this conclusory claim is not supported by any facts at all—and Plaintiffs' own allegations contradict this claim. *See* CAC ¶ 68 (acknowledging Link makes clear "credentials will never be made accessible to Venmo."). Thus, Plaintiffs have not plausibly alleged that Plaid transferred access tokens or login credentials "*to another*," thereby failing to state a claim under § 1030(a)(6). *See Oracle Am., Inc. v. TERiX Computer Co., Inc.*, No. 5:13-CV-03385-PSG, 2014 WL 31344, at *6 (N.D. Cal. Jan. 3, 2014).

Plaintiffs allege no virus or computer contaminant claim under § 1030(a)(5)(A) or § 502(c)(8). Finally, Plaintiffs fail to state a claim under these statutes' computer virus provisions. 18 U.S.C. § 1030(A)(5)(A) (criminalizing the "transmission of a program, information, code, or command" that "intentionally causes damage without authorization, to a protected computer."); Cal.

Penal Code § 502(c)(8), (b)(12) (prohibiting introduction of a "contaminant" like "viruses or worms that" "modify, damage, destroy, record, or transmit information within" a computer). These laws are "aimed at 'viruses or worms,' and other malware that usurps the normal operation of the computer or computer system." *In re iPhone Application Litig.*, 2011 WL 4403963, at *13. While Plaintiffs say Plaid "impaired the integrity of Plaintiffs' and Class members' smartphones by installing software within the Participating Apps that captured their sensitive bank login data," this does "not impair the integrity or availability of" data or systems (*Fidlar*, 810 F.3d at 1084), nor are Plaid's integrations anything like "viruses or worms." *See In re iPhone Application Litig.*, 2011 WL 4403963, at *13.

For all the above reasons, it is clear Plaintiffs have not made allegations even approaching a plausible CFAA or CDAFA claim, and these claims must be dismissed.

4. Plaintiffs fail to plead a plausible claim under the SCA.

The SCA "aims to prevent hackers from obtaining, altering or destroying certain stored electronic communications." *In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d 497, 507 (S.D.N.Y. 2001). To establish their claim, Plaintiffs must allege facts showing Plaid: (1) "intentionally accesse[d] without authorization," or "exceed[ed] an authorization to access," (2) "a facility through which an electronic communication service is provided," and (3) "thereby obtain[ed], alter[ed], or prevent[ed] authorized access to a wire or electronic communication while it [was] in electronic storage in such system." 18 U.S.C. § 2701(a). Plaintiffs conclusorily allege their financial institutions are "facilities" under the SCA, and that Plaid accessed "electronic communications" without or in excess of authorization while those communications were stored "for [the] purposes of backup protection." CAC ¶¶ 302, 305, 307-308. These allegations fail as a matter of law.

First, a financial institution is not "a facility through which an electronic communication service is provided" because it "is not an internet service provider or analogous to one." *Cent. Bank & Tr. v. Smith*, 215 F. Supp. 3d 1226, 1234-35 (D. Wy. 2016). Plaintiffs' argument "attempt[s] to put a square peg of facts in a round hole of law." *Id.* at 1134. Courts in this District have refused to expand the scope of "a facility" beyond "the computer systems of an email provider, a bulletin board system, or an ISP," none of which are alleged in the CAC. *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1057 (declining to expand meaning of facility to "an individual's computer, laptop, or

mobile device"); *see also Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1041 (N.D. Cal. 2014) ("mobile devices cannot be 'facilities'").

Second, Plaintiffs do not sufficiently allege Plaid accessed an "electronic communication" under § 2701(a). Plaintiffs concede—as they must, given the definitional exclusion in § 2510(12)—that, "[f]or [the] purposes of [their SCA] cause of action only, the communications at issue exclude any electronic funds transfer ["EFT"] information stored by a financial institution." CAC ¶ 304. But Plaintiffs fail to allege Plaid accessed non-EFT information. While Plaintiffs suggest that "[f]inancial institutions necessarily store historical communications" and "historical direct messages" (CAC ¶ 305), they do not allege Plaid accessed these communications. Because Plaintiffs do not state "enough facts to state a claim to relief that is plausible on its face," this claim fails for this independent reason, as well.[25] *See Twombly*, 550 U.S. at 570; *Iqbal*, 556 U.S. at 678.

Third, Plaintiffs do not plausibly allege Plaid accessed an electronic communication "while it [was] in electronic storage." 18 U.S.C. § 2701(a). In relevant part, "electronic storage" means "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(B). Plaintiffs' claim fails because, while they allege "[f]inancial institutions necessarily store historical communications" (CAC ¶¶ 305, 307), they do not allege Plaid *accessed* any "historical communications," let alone while they were in "storage"—*i.e.*, "for purposes of backup protection." *See Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1044 (N.D. Cal. 2018) (dismissing claim because communications were emails on a web server, not backups); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1076 (9th Cir. 2004) ("[t]he mere fact that a copy *could* serve as a backup does not mean it is stored for that purpose.").

Finally, Plaintiffs cannot plausibly allege Plaid accessed data without or in excess of authorization, let alone that Plaid did so intentionally. The SCA's definition of authorization is comparable to the definition in the CFAA and only prohibits unauthorized "access"—not use of data

[25] Nor do Plaintiffs allege Plaid accessed any "transfer" of electronic data that was "transmitted" from a Plaintiff to any intended recipient. *See* 18 U.S.C. § 2510(12) (defining "electronic communication" as "*any transfer* [of electronic data] of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system" (emphasis added)); *see also Rene v. G.F. Fishers, Inc.*, 817 F. Supp. 2d 1090, 1093 (S.D. Ind. 2011) ("Defendants correctly point out than an electronic communication within the purview of the statute must be transmitted by a system").

once it has been accessed. *See* 18 U.S.C. § 2701; *Stern v. Weinstein*, 512 F. App'x 701, 702 (9th Cir. 2013) (no SCA violation "even if [defendant] violated restrictions on the use of the information he accessed") (mem. dispo.); *Cent. Bank & Tr.*, 215 F. Supp. 3d at 1236 (same). Thus, Plaintiffs' claim that Plaid violated the SCA "by collecting, aggregating, selling, and divulging … electronic banking communications" (CAC ¶ 308) fails as a matter of law because these claims relate to the "use" of data, not the "access" to data. Any data Plaid allegedly *accessed* was accessed with Plaintiffs' authorization and at their request. Any claim to the contrary is not plausible in light of Plaid's Privacy Policy, the privacy policies and terms of the apps used by end users, and Plaintiffs' stated purpose for using the apps. *Supra*, at 3-7, 18-19; CAC ¶ 100; *Cent. Bank & Trust*, 215 F. Supp. 3d at 1235-36. For each of the above independent reasons, the Plaintiffs' SCA claim should be dismissed.

5. Plaintiffs fail to plead invasion of privacy or violation of California's constitution.

"The California Constitution and the common law both set a high bar for an invasion of privacy claim." *Belluomini v. Citigroup, Inc.*, No. CV 13-01743 CRB, 2013 WL 3855589, at *6 (N.D. Cal. July 24, 2013). Courts typically assess the two claims together since the elements are "largely parallel." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 288 (2009). Plaintiffs must demonstrate (1) a legally protected privacy interest, reasonable under the circumstances, and (2) that any invasion of privacy was "sufficiently serious … to constitute an egregious breach of the social norms underlying the privacy right." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 37, 39-40 (1994). Plaintiffs allege Plaid invaded their privacy by improperly accessing and using their financial data (CAC ¶¶ 262, 344), but these allegations are not plausible for numerous reasons.

First, Plaintiffs cannot plausibly allege a reasonable expectation of privacy given: (1) their choice to link their accounts to their chosen apps, (2) (assuming Plaintiffs even linked through Plaid) Plaid's Privacy Policy, (3) the privacy policies and terms of the apps used by end users, and (4) the fact that they have not alleged taking any action to stop the alleged invasion by disconnecting their accounts or asking Plaid to delete their data. *Supra*, at 4-7; *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1037-38 (N.D. Cal. 2014) ("The plaintiff in an invasion of privacy action must … not have manifested by his or her conduct a voluntary consent to the invasive action of defendant."). "[T]he presence or absence of opportunities to consent voluntarily to activities impacting privacy interests

obviously affects the [reasonable] expectations of the participant." *Hill*, 7 Cal. 4th at 37. Far from acting "consistent[ly] with an actual expectation of privacy[,]" Plaintiffs "manifested by [their] conduct a voluntary consent to" the complained-of practices. *See Gonzales*, 305 F. Supp. 3d at 1091.

Second, Plaintiffs admit that Plaid's Privacy Policy discloses the information Plaid collects, yet they inexplicably (and insufficiently) assert an expectation of privacy in that very information. *Compare* CAC ¶¶ 261, 341 ("Plaintiffs and Class members reasonably expected that their login credentials, account numbers, balances, transaction history, and other information was private and secure within the banks at which they maintain accounts") *with* CAC ¶ 71 (admitting Plaid's Privacy Policy discloses collection of account numbers, balances, transactions, and other information). Courts routinely hold that when data collection practices are disclosed to end users, as they have been here, there is no reasonable expectation of privacy. *See*, *e.g.*, *TBG Ins. Servs. Corp.*, 96 Cal. App. 4th at 452 (advance notice in the company's policy statement gave "the opportunity to consent to or reject the very thing that [plaintiff] now complains about"); *Berry v. Webloyalty.com, Inc.*, No. 10-CV-1358-H CAB, 2011 WL 1375665, at *10 (S.D. Cal. Apr. 11, 2011), *vacated and remanded on other grounds*, 517 F. App'x 581 (9th Cir. 2013) (dismissing privacy claims because "there is no reasonable expectation of privacy" in light of consent[26] to share information).

Third, Plaintiffs' allegations do not show an "egregious breach of the social norms." *Hill*, 7 Cal. 4th at 37. To assess egregiousness, courts consider "all of the surrounding circumstances, including the degree and setting of the intrusion and the intruder's motives and objectives." *Hernandez*, 47 Cal. 4th at 295 (quotation marks omitted) (finding no sufficiently serious invasion of privacy where employer surreptitiously videotaped employees in their office). Courts routinely hold that disclosure of personal or financial information, without more, is not an egregious breach of social norms sufficient to establish invasion of privacy. *See*, *e.g.*, *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012); *Folgelstrom v. Lamps Plus, Inc*., 195 Cal. App. 4th 986, 992 (2011). Certainly, Plaintiffs do not sufficiently allege any such breach in this case. Instead, to the extent

[26] In *Berry*, the website instructed the plaintiff to enter his email address and click "Yes" to sign up for a membership program. *Id*. at *4. It provided that "[b]y entering my email address as my electronic signature and clicking YES, I have read and agree to the Offer and Billing Details and authorize MovieTickets.com to securely transfer my name, address and credit or debit card information to Shopper Discounts & Rewards for billing and benefit processing." *Id*.

Plaid was even used to link Plaintiffs' accounts, Plaid acted entirely in accordance with its Privacy Policy and with the Plaintiffs' choice in connecting their chosen apps with their financial accounts.

Plaintiffs' allegations that Plaid's Privacy Policy is not conspicuous enough and its security protocols may not mirror those of banks (CAC ¶¶ 57-62, 153, 232)—even taking those allegations as true—are not enough to constitute an "egregious breach." *See Razuki v. Caliber Home Loans, Inc.*, No. 17cv1718-LAB (WVG), 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018) (allegations that defendant "intentionally violated his privacy [with] low-budget security measures … don't suggest the type of intentional, egregious privacy invasion contemplated in *Hill*," even after breach exposed sensitive customer information, including social security numbers); *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063 ("Even negligent conduct that leads to theft of highly personal information, including social security numbers, does not … constitute a violation of Plaintiffs' right to privacy."). And just as users can choose to link their banks to their apps, they can choose to stop doing so. Venmo tells users they can always "turn off Venmo's use of Plaid," and Plaid will delete users' data upon request. Yet not a single Plaintiff claims to have done either of these things, making plain that they do not consider the alleged "invasion of privacy" to be "egregious." *Supra*, at 6-7.

6. Plaintiffs fail to plead a plausible claim under the California Anti-Phishing Act.

The Anti-Phishing Act prohibits use of the internet "to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business." Cal. Bus. & Prof. Code § 22948.2. The law's intent is to criminalize phishing—which involves using fraudulent emails or websites to trick consumers into providing personal information to what look like legitimate companies (but are not), and then using that information to facilitate identity theft and other crimes. Cal. Bill Anal., S.B. 355 Assem., July 13, 2005; Cal. Bill Anal., S.B. 355 Sen., July 5, 2005.

This law does not apply to Plaid—which provides valuable services to end users at their request and with their permission. Given the services Plaid provides in enabling end users to connect their financial accounts to their chosen apps, the disclosures in Plaid Link, Plaid's Privacy Policy and the privacy policies and terms of the apps used by end users, as well as Plaintiffs' apparent continued use of Plaid, Plaintiffs cannot plausibly allege that Plaid is not a "legitimate" company, that Plaid

tricked Plaintiffs into disclosing their information, or that they suffered harm because of Plaid. *Supra*, at 3-7, 18-19. Nor can Plaintiffs allege Plaid's goal in "obtaining personal information" is "to facilitate identity theft and other crimes." *See* Cal. Bill Anal., S.B. 355 Sen., July 5, 2005. Indeed, Plaintiffs concede "[t]he primary service offered by Plaid … is bank 'linking' and verification" to facilitate financial transactions. CAC ¶ 32. Additionally, Plaintiffs do not allege Plaid "represent[ed] itself to be a business without the authority or approval *of the business*" (Cal. Bus. & Prof. Code § 22948.2 (emphasis added)), as the claim that Plaid acted "without obtaining the authority or approval of each financial institution" (CAC ¶ 353) is not factually supported and should be disregarded. *See Twombly*, 550 U.S. at 555; *Iqbal*, 556 U.S. at 678-80; *Adams*, 355 F.3d at 1183; *Johnson v. Riverside Healthcare Sys., LP*, 534 F.3d 1116, 1122 (9th Cir. 2008).

7. Plaintiffs fail to plead a plausible claim for deceit.

Plaintiffs allege "Plaid engaged in deceit by intentionally concealing and failing to disclose its true nature and conduct to consumers." CAC ¶ 360. To establish such a claim under Civil Code § 1710(3), Plaintiffs must plead with particularity: "(1) concealment or suppression of material fact, (2) a duty to disclose the fact to the plaintiff, (3) intentional concealment with intent to defraud, (4) justifiable reliance, and (5) resulting damages." *Lewis*, 2020 WL 2745253, at *14. Plaintiffs allege none of these elements, let alone with the requisite specificity.[27] *London v. New Albertson's, Inc.*, No. 08-CV-1173 H (CAB), 2008 WL 4492642, at *8 (S.D. Cal. Sept. 30, 2008) (dismissing deceit claims for "fail[ure] to allege with particularity the times, places, and those involved in the alleged non-disclosure of material facts" required by Rule 9(b)).[28]

[27] Since Plaintiffs' attempt to plead deceit focuses on alleged misrepresentations in Plaid Link, Plaintiffs' claims in connection with apps, such as Cash App, that they say "do not even make use of the template and provide no disclosures whatsoever" cannot form the basis for this theory of liability at all. *See* CAC ¶ 66.

[28] For claims sounding in fraud, Fed. R. Civ. P. 9(b) requires allegations of "the 'who, what, when, and where' of the allegedly fraudulent statements." *Lindberg v. Wells Fargo Bank N.A.*, No. CV C 13-0808 PJH, 2013 WL 3457078, at *4 (N.D. Cal. July 9, 2013); *Desaigoudar v. Meyercord*, 223 F.3d 1020, 1022-1023 (9th Cir. 2000) (fraud must be pled "with a high degree of meticulousness"). While claims based on an alleged fraudulent omission or concealment "can succeed without the same level of specificity required by a normal fraud claim" (*see Baggett v. Hewlett Packard Co.,* 582 F. Supp. 2d 1261, 1267 (C.D. Cal. 2007)), "the contention that … nondisclosure claims need not be pleaded with particularity is unavailing." *Kearns*, 567 F.3d at 1127. A plaintiff "must describe the content of the omission and where the omitted information should or could have been revealed, as well as provide representative samples of advertisements, offers, or other representations that plaintiff

First, as discussed at length in Section III. B, *supra*, Plaintiffs cannot plausibly or specifically allege concealment of a material fact. The ten "facts" Plaintiffs allege were concealed (or that Plaid failed to disclose), are not omissions at all, but instead are contradicted by express disclosures contained in the Privacy Policy. Plaintiffs thus cannot establish the most basic requirement of their deceit claim.

Second, Plaintiffs have not alleged Plaid has a legally enforceable duty in these circumstances. Nondisclosure or concealment can only constitute actionable fraud when there exists a fiduciary relationship or "some other relationship between the plaintiff and defendant in which a duty to disclose can arise." *Hoffman v. 162 N. Wolfe LLC*, 228 Cal. App. 4th 1178, 1186-87 (2014), *as modified on denial of reh'g* (Aug. 13, 2014). Here, while Plaintiffs conclusorily allege that Plaid was "under a duty to disclose" (CAC ¶ 360), Plaintiffs do not allege there was any transaction between them and Plaid giving rise to a duty to disclose, since they do not allege any "act or agreement" altering the legal relations between themselves and Plaid. *See Planned Parenthood Fed'n of Am., Inc. v. Ctr. for Med. Progress*, 402 F. Supp. 3d 615, 683, 727 (N.D. Cal. 2019). Indeed, this type of relationship is typically "between seller and buyer, employer and prospective employee, doctor and patient, or parties entering into any kind of contractual agreement"—not between parties like Plaintiffs and Plaid. *See Hoffman*, 228 Cal. App. 4th at 1187. To be clear, Plaid disclosed the information Plaintiffs allege was concealed, but Plaintiffs do not adequately allege a duty giving rise to liability.[29]

Third, Plaintiffs fail to plausibly or specifically allege Plaid intentionally concealed any fact with an intent to defraud. *O'Hara v. W. Seven Trees Corp.*, 75 Cal. App. 3d 798, 804, (1977) ("a plaintiff must allege a misrepresentation made with knowledge of its falsity and with the intent to

---

relied on to make her purchase and that failed to include the allegedly omitted information." *Marolda v. Symantec Corp.*, 672 F. Supp. 2d 992, 1002 (N.D. Cal. 2009).

[29] Plaintiffs' claim also fails because, while "[a] defendant must exercise 'reasonable care' to bring the information to the plaintiff's attention when under such a duty … '[i]f reasonable care is exercised, the fact that the information does not reach the person entitled to it does not subject [the defendant] to liability.'" *Sloan v. Gen. Motors LLC*, 287 F. Supp. 3d 840, 873-74 (N.D. Cal. 2018) (citing Rest. (Second) of Torts § 551, cmt. on Subsect. (2) (1977)). As in *Sloan*, "Plaintiffs are missing [] a plausible allegation that they would have received the information if disclosed through [] various channels of information" when Plaid plainly exercised "reasonable care" to disclose their Privacy Policy to end users like Plaintiffs. *See id*. at 875.

defraud, *i.e.*, to induce reliance"). As discussed at length herein, Plaid's Privacy Policy expressly discloses how Plaid collects and uses data, and Plaid Link includes reference to Plaid's Privacy Policy, which demonstrates Plaid concealed nothing, let alone with intent to defraud. *Supra*, at 4-7. Plaintiffs' conclusory and implausible allegations are undercut by the clear disclosures provided in Plaid Link and should be disregarded. *See Twombly*, 550 U.S. at 570; *Iqbal*, 556 U.S. at 678.

Fourth, Plaintiffs fail to specifically allege reasonable reliance. Plaintiffs do not allege they *saw* any statements made by Plaid, let alone that they justifiably relied on any such statements. Indeed, Plaintiffs' tactics are exposed by comparing the allegations in the original Complaint (ECF No. 1) with those in the CAC.[30] Mr. Cottle, for example, admitted he does not "recall[] specific details regarding the process of logging into his bank account in the Venmo app" (ECF No. 1 ¶ 112), but now claims, "[t]o the extent" he "recalls specific details about the process of linking his bank account to his Venmo account … those details are consistent with the discussion of Plaid's interface herein" (CAC ¶ 112). All Plaintiffs make the same vague claim. CAC ¶¶ 101, 112, 122, 131, 141, 151, 160, 169, 179, 190, 200. A "plaintiff cannot demonstrate reasonable reliance on an alleged omission when the purportedly omitted fact is disclosed." *Lewis*, 2020 WL 2745253, at *14; *see also Dix v. Nova Benefit Plans, LLC*, CV 14-08678-AB (FFMx), 2015 WL 12859221, at *7 (C.D. Cal. Apr. 28, 2015) ("A plaintiff cannot claim justifiable reliance where, as here, 'disclaimers … are more than sufficient to put a reasonably prudent [plaintiff] on notice …."); *Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1163-64 (9th Cir. 2012) (finding no justifiable reliance on purported failure to disclose annual fee because fee was disclosed in terms to which plaintiff agreed); *Circle Click Media LLC v. Regus Mgmt. Grp. LLC*, No. 12-04000 SC, 2013 WL 57861, at *11 (N.D. Cal. Jan. 3, 2013) (same). Plaid's Privacy Policy contains express disclosures that undercut all of Plaintiffs' claims.

Finally, Plaintiffs fail to allege damage as required under § 1709. *Supra*, at 8-12. Each of these reasons independently requires dismissal of Plaintiffs' deceit claim.

[30] *Azadpour v. Sun Microsystems, Inc.*, No. C06-03272 MJJ, 2007 WL 2141079, at *2 n.2 (N.D. Cal. July 23, 2007) ("Where allegations in an amended complaint contradict those in a prior complaint, a district court need not accept the new alleged facts as true, and may, in fact, strike the changed allegations as false.") (citations omitted).

8. Plaintiffs fail to state a claim for unjust enrichment.

Plaintiffs' unjust enrichment "claim" fails because they have available (and allege) an adequate remedy at law (*supra*, at Section IV. C), and for two additional independent reasons. *First*, "unjust enrichment is a remedy and not an independent claim" and therefore must be "dismissed with prejudice." *McLellan v. Fitbit, Inc.*, No. 3:16-cv-00036-JD, 2018 WL 2688781, at *4 (N.D. Cal. June 5, 2018). *Second*, even if the Court construed their claim as a quasi-contract restitution claim, it would still fail. While "[r]estitution may be available where the defendant obtained a benefit from the plaintiff by fraud, duress, conversion, or similar conduct … when [as here and discussed above] a plaintiff fails to sufficiently plead an actionable misrepresentation or omission, his or her restitution claim must be dismissed." *Rojas-Lozano v. Google, Inc.*, 159 F. Supp. 3d 1101, 1120 (N.D. Cal. 2016) (internal citation and quotations omitted).

9. Plaintiffs' declaratory and injunctive relief claims fail.

Plaintiffs assert claims for declaratory and injunctive relief, but both should be dismissed because Plaintiffs have an adequate remedy at law (*supra*, at Section IV. C), and because they are equitable remedies, not causes of action. *See Curtis v. Option One Mortg. Corp.*, No. 1:09-CV-1982 AWIS MS, 2010 WL 1729770, at *8 (E.D. Cal. Apr. 28, 2010) ("an injunction is a remedy to another claim or cause of action and not a claim or cause of action in and of itself."); *Skelly Oil Co. v. Phillips Petroleum Co.* 339 U.S. 667, 671 (1950) (same, regarding declaratory relief). Additionally, Plaintiffs' request for a declaratory judgment that Plaid "otherwise improperly used Plaintiffs' private data" necessarily derives from and depends on Plaintiffs' other causes of action. Because those claims fail (*supra*, at Sections IV. D. 1-7), this derivative claim also fails and should be dismissed. *See Jackson v. Atl. Sav. of Am.*, No. 13-cv-05755-CW, 2014 WL 4802879, at *3-4 (N.D. Cal. Sept. 26, 2014); *Ctr. for Sci. in Pub. Interest v. Bayer Corp.*, No. C 09-05379 JSW, 2010 WL 1223232, at *4 (N.D. Cal. Mar. 25, 2010). In any event, declaratory relief "should not be granted where a special statutory proceeding has been provided," which can determine the rights and duties of the parties. *Katzenbach v. McClung*, 379 U.S. 294, 296 (1964). Because statutory remedies are "more appropriate" (though meritless on other grounds), declaratory relief should be denied. *Smith v.*

Metropolitan Property & Liab. Ins. Co., 629 F.2d 757, 759 (2nd Cir. 1980); *see also Simmons First Nat'l Bank v. Lehman*, No. 13-CV-02876-DMR, 2015 WL 1503437, at *7 (N.D. Cal. Apr. 1, 2015).

E. Plaintiffs' CAC should be dismissed with prejudice.

Plaintiffs' CAC should be dismissed with prejudice because Plaintiffs' claims are legally defective and cannot be cured by amendment. *See*, *e.g.*, *Sisseton-Wahpeton Sioux Tribe v. United States*, 90 F.3d 351, 356 (9th Cir. 1996); *Low*, 900 F. Supp. 2d at 1033 (dismissing SCA and unjust enrichment claims with prejudice on this basis); *McLellan*, 2018 WL 2688781, at *4 (dismissing unjust enrichment claim with prejudice because it "is a remedy and not an independent claim."). Plaintiffs already had more than ample opportunity to amend their complaint. After filing an initial 85-page complaint, they banded together with many additional counsel and plaintiffs who had filed four separate complaints, and prepared their 112-page CAC. If Plaintiffs could not come up with a viable claim with 12 law firms, 19 named plaintiffs (some of whom were dropped from the CAC), and 112 pages of allegations, they will not be able to do so in the future. This is essentially Plaintiffs' sixth bite at the apple, amendment would be futile, and the CAC should be dismissed in full with prejudice. *See Berkeley v. Wells Fargo Bank*, No. 15-CV-00749-JSC, 2016 WL 67221, at *12 (N.D. Cal. Jan. 6, 2016) (dismissing complaint with prejudice "given Plaintiff's multiple opportunities to amend [such that] another opportunity … would be futile."); *Carter v. Bank of Am., N.A.*, No. EDCV-15-1474-MWF (DTBx), 2016 WL 6571264, at *4 (C.D. Cal. Jan. 20, 2016) ("the Court refuses to allow Plaintiffs essentially a fifth bite at the apple because amendment appears to be futile.").

V. CONCLUSION

Plaid respectfully requests that this Court dismiss Plaintiffs' CAC without leave to amend.

Dated: September 14, 2020

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

/s/ Ethan D. Dettmer
By: Ethan D. Dettmer

Attorneys for Defendant Plaid Inc.